西安电子科技大学
XIDIAN UNIVERSITY

具有最大弯曲分量数的二次二项式

张神星 (合肥工业大学)

2026 年西电 *4* 月数论线上会议

本文与谢贤红、欧阳毅合作完成

zhangshenxing@hfut.edu.cn

https://faculty.hfut.edu.cn/zhangshenxing

向量函数

设 $n = 2m$ 为偶数, $\mathbb{F}_{2^n}$ 为 2^n 元有限域.

向量函数

component function

设 $n = 2m$ 为偶数, $\mathbb{F}_{2^n}$ 为 2^n 元有限域. 考虑函数 $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, 其分量函数为

$$F_a(v) = \mathrm{Tr}_{2^n/2}\big(a \cdot F(v)\big), \quad a \in \mathbb{F}_{2^n},$$

向量函数

component function

设 $n = 2m$ 为偶数, $\mathbb{F}_{2^n}$ 为 2^n 元有限域. 考虑函数 $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, 其分量函数为

$$F_a(v) = \mathrm{Tr}_{2^n/2}\big(a \cdot F(v)\big), \quad a \in \mathbb{F}_{2^n},$$

对应的 **Walsh 变换**为:

$$W_{F_a}(\omega) = \sum_{v \in \mathbb{F}_{2^n}} (-1)^{F_a(v) + \mathrm{Tr}_{2^n/2}(\omega v)} = \sum_{v \in \mathbb{F}_{2^n}} \psi\big(aF(v) + \omega v\big).$$

其中 $\psi(x) = (-1)^{\mathrm{Tr}_{2^n/2}(x)}$ 为加性特征.

向量函数

设 $n = 2m$ 为偶数, $\mathbb{F}_{2^n}$ 为 2^n 元有限域. 考虑函数 $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, 其**分量函数**(component function)为

$$F_a(v) = \mathrm{Tr}_{2^n/2}\big(a \cdot F(v)\big), \quad a \in \mathbb{F}_{2^n},$$

对应的 **Walsh 变换**为:

$$W_{F_a}(\omega) = \sum_{v \in \mathbb{F}_{2^n}} (-1)^{F_a(v) + \mathrm{Tr}_{2^n/2}(\omega v)} = \sum_{v \in \mathbb{F}_{2^n}} \psi\big(aF(v) + \omega v\big).$$

其中 $\psi(x) = (-1)^{\mathrm{Tr}_{2^n/2}(x)}$ 为加性特征.

若对所有 ω 均有 $W_{F_a}(\omega) = \pm 2^m$, 则 F_a 是**弯曲分量**(bent component).

定理 (Pott 等, 2018)

$\#S_F \geqslant 2^m$, 其中

$$S_F = \{a : F_a \text{ 不是弯曲分量}\} \subseteq \mathbb{F}_{2^n}.$$

等号成立当且仅当 S_F 是 m 维子空间.

已有结果

定理 (Pott 等, 2018)

$\#S_F \geqslant 2^m$, 其中

$$S_F = \{a : F_a \text{ 不是弯曲分量}\} \subseteq \mathbb{F}_{2^n}.$$

等号成立当且仅当 S_F 是 m 维子空间.

我们称具有 $2^n - 2^m$ 个弯曲分量的函数为具有最大弯曲分量数.

定理 (Pott 等, 2018)

$\#S_F \geqslant 2^m$, 其中

$$S_F = \{a : F_a \text{ 不是弯曲分量}\} \subseteq \mathbb{F}_{2^n}.$$

等号成立当且仅当 S_F 是 m 维子空间.

我们称具有 $2^n - 2^m$ 个弯曲分量的函数为具有最大弯曲分量数.

不难知道, $S_{F^2} = (S_F)^2$. 从而仅相差 Frobenius 作用的 (称之为仿射等价 (affine equivalent)) 多项式具有相同的弯曲分量数.

定理 (Pott 等, 2018)

$\#S_F \geqslant 2^m$, 其中

$$S_F = \{a : F_a \text{ 不是弯曲分量}\} \subseteq \mathbb{F}_{2^n}.$$

等号成立当且仅当 S_F 是 m 维子空间.

我们称具有 $2^n - 2^m$ 个弯曲分量的函数为具有最大弯曲分量数.

不难知道, $S_{F^2} = (S_F)^2$. 从而仅相差 Frobenius 作用的 (称之为仿射等价 (affine equivalent)) 多项式具有相同的弯曲分量数.

- 单项式中只有 $x^{2^i(2^m+1)}$ 达到最大值 (胡红刚等, 2023).

已有结果

定理 (Pott 等, 2018)

$\#S_F \geqslant 2^m$, 其中

$$S_F = \{a : F_a \text{ 不是弯曲分量}\} \subseteq \mathbb{F}_{2^n}.$$

等号成立当且仅当 S_F 是 m 维子空间.

我们称具有 $2^n - 2^m$ 个弯曲分量的函数为具有最大弯曲分量数.

不难知道, $S_{F^2} = (S_F)^2$. 从而仅相差 Frobenius 作用的 (称之为仿射等价 (affine equivalent)) 多项式具有相同的弯曲分量数.

- 单项式中只有 $x^{2^i(2^m+1)}$ 达到最大值 (胡红刚等, 2023).
- 二项式 $x^{2^i+1} + x^{2^i+2^m}$ 达到最大值 (Pott 等, 2018).

已有结果

定理 (Pott 等, 2018)

$\#S_F \geqslant 2^m$, 其中

$$S_F = \{a : F_a \text{ 不是弯曲分量}\} \subseteq \mathbb{F}_{2^n}.$$

等号成立当且仅当 S_F 是 m 维子空间.

我们称具有 $2^n - 2^m$ 个弯曲分量的函数为具有最大弯曲分量数.

不难知道, $S_{F^2} = (S_F)^2$. 从而仅相差 Frobenius 作用的 (称之为仿射等价 (affine equivalent)) 多项式具有相同的弯曲分量数.

- 单项式中只有 $x^{2^i(2^m+1)}$ 达到最大值 (胡红刚等, 2023).
- 二项式 $x^{2^i+1} + x^{2^i+2^m}$ 达到最大值 (Pott 等, 2018).
- 对于 $x^{2^i+1} + x^{2^m+1}$, 仅当 $i = 0$ 时达到最大值 (谢贤红等, 2025).

具有最大弯曲分量的二次二项式

设 $N = 2^n - 1$, $\mathrm{wt}_2(d)$ 为 $d \bmod N$ 的二进制分量个数 (即汉明权重 (Hamming weight)).

具有最大弯曲分量的二次二项式

Hamming weight

设 $N = 2^n - 1$, $\mathrm{wt}_2(d)$ 为 $d \bmod N$ 的二进制分量个数 (即汉明权重).

我们想要研究 $F(x) = x^{d_1} + x^{d_2}$ 的情形, 其中 $\mathrm{wt}_2(d_1), \mathrm{wt}_2(d_2) \leqslant 2$.

具有最大弯曲分量的二次二项式

Hamming weight

设 $N = 2^n - 1$, $\mathrm{wt}_2(d)$ 为 $d \bmod N$ 的二进制分量个数 (即汉明权重).

我们想要研究 $F(x) = x^{d_1} + x^{d_2}$ 的情形, 其中 $\mathrm{wt}_2(d_1), \mathrm{wt}_2(d_2) \leqslant 2$. 设 $\sigma(x) = x^2$ 为 Frobenius, 设 $s := \gcd(d_1, d_2, 2^m - 1)$,

$$\ell(n) := \min_{\mathbb{F}_2(\gamma)=\mathbb{F}_{2^n}} \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma.$$

具有最大弯曲分量的二次二项式

设 $N = 2^n - 1$, $\mathrm{wt}_2(d)$ 为 $d \bmod N$ 的二进制分量个数 (即汉明权重 Hamming weight).

我们想要研究 $F(x) = x^{d_1} + x^{d_2}$ 的情形, 其中 $\mathrm{wt}_2(d_1), \mathrm{wt}_2(d_2) \leqslant 2$. 设 $\sigma(x) = x^2$ 为 Frobenius, 设 $s := \gcd(d_1, d_2, 2^m - 1)$,

$$\ell(n) := \min_{\mathbb{F}_2(\gamma)=\mathbb{F}_{2^n}} \dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma.$$

定理

假设 $\ell(n) > m$, $s > 1$. 若 $F(x) = x^{d_1} + x^{d_2}$ 具有最大弯曲分量数, 则 $S_F = \mathbb{F}_{2^m}$ 且 $d_2 - d_1 \equiv 0 \bmod 2^m - 1$. 而且,

(1) **若 $\mathrm{wt}_2(d_1) = 1$, 则 F 等价于 x^{2^m+1};** *(相差线性函数也不改变弯曲分量数)*

(2) **若 $\mathrm{wt}_2(d_1) = \mathrm{wt}_2(d_2) = 2$, 则 F 仿射等价于 $x^{2^i+1} + x^{2^i+2^m}$.**

关于非线性度和差分均匀度, 我们有如下较为一般的估计:

定理

假设 $\ell(n) > m$, $\sigma \circ F = F \circ \sigma$. 若 F 具有最大弯曲分量数, 则

$$\text{非线性度 } \mathcal{N}_F := 2^{n-1} - \frac{1}{2} \max_{a \neq 0, \omega} |W_{F_a}(\omega)| \leqslant 2^{n-1} - \frac{1}{2} \sqrt{\frac{2^{3m}}{T} \left(\frac{2^{3m}}{\#\operatorname{Im}(F)} - 2^{m+1} + 1 \right)},$$

$$\text{差分均匀度 } \delta_F := \max_{a \neq 0, b} \#\{x : F(x+a) + F(x) = b\} \geqslant \left\lceil \frac{2^n}{\#\Delta} \left(\frac{2^n}{\#\operatorname{Im}(F)} - 1 \right) \right\rceil,$$

其中

$$T = \#\{a \in \mathbb{F}_{2^m}^* : W_{F_a}(0) \neq 0\},$$

$$\Delta = \{x + y : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n},\ x \neq y,\ F(x) = F(y)\}.$$

对于 $F(x) = x^{2^l+1} + x^{2^l+2^m}$, 我们有:

定理

设 $F(x) = x^{2^l+1} + x^{2^l+2^m}$.

(1) $\delta_F \geqslant 2^m$.

(2) 若 $v_2(m) \leqslant v_2(l)$, 则 $\mathcal{N}_F \leqslant 2^{n-1} - 2^{m-1}$.

(3) 若 $v_2(m) > v_2(l)$, 则 $\mathcal{N}_F \leqslant 2^{n-1} - 2^{\frac{3m}{2}+d-1}$, 其中 $d = \gcd(l, m)$.

(1) 由假设条件 $\ell(n) > m$ 可知 $S_F \setminus \mathbb{F}_{2^m}$ 中元素必落在 $\mathbb{F}_{2^n}$ 真子域中, 通过大小关系得到该集合必定为空, 从而 $S_F = \mathbb{F}_{2^m}$.

主要思路

(1) 由假设条件 $\ell(n) > m$ 可知 $S_F \setminus \mathbb{F}_{2^m}$ 中元素必落在 $\mathbb{F}_{2^n}$ 真子域中, 通过大小关系得到该集合必定为空, 从而 $S_F = \mathbb{F}_{2^m}$.

(2) 利用高斯和对 $W_{F_a}(b)$ 作 2 进展开, 得到它的 2 赋值最小值为 m. 通过分析首项作为 a, b 的多项式的零点数量, 得到存在 $d_1 j_1 + d_2 j_2 \equiv 0, j_1 + j_2 \equiv 2^n - 2^m \bmod N$.

主要思路

(1) 由假设条件 $\ell(n) > m$ 可知 $S_F \setminus \mathbb{F}_{2^m}$ 中元素必落在 $\mathbb{F}_{2^n}$ 真子域中, 通过大小关系得到该集合必定为空, 从而 $S_F = \mathbb{F}_{2^m}$.

(2) 利用高斯和对 $W_{F_a}(b)$ 作 2 进展开, 得到它的 2 赋值最小值为 m. 通过分析首项作为 a, b 的多项式的零点数量, 得到存在 $d_1 j_1 + d_2 j_2 \equiv 0, j_1 + j_2 \equiv 2^n - 2^m \bmod N$.

(3) 比较 wt_2 得到 $j_1 = 2^m j, j_2 = 2^m(2^m - 1 - j)$.

主要思路

(1) 由假设条件 $\ell(n) > m$ 可知 $S_F \setminus \mathbb{F}_{2^m}$ 中元素必落在 $\mathbb{F}_{2^n}$ 真子域中, 通过大小关系得到该集合必定为空, 从而 $S_F = \mathbb{F}_{2^m}$.

(2) 利用高斯和对 $W_{F_a}(b)$ 作 2 进展开, 得到它的 2 赋值最小值为 m. 通过分析首项作为 a, b 的多项式的零点数量, 得到存在 $d_1 j_1 + d_2 j_2 \equiv 0, j_1 + j_2 \equiv 2^n - 2^m \bmod N$.

(3) 比较 wt_2 得到 $j_1 = 2^m j, j_2 = 2^m(2^m - 1 - j)$.

(4) 由陪集分解可知, 当 $s = \gcd(d_1, d_2, N) > 1$ 时, $s \mid (2^m \pm 1) \iff W_{F_a}(0) = \mp 2^m$.

主要思路

(1) 由假设条件 $\ell(n) > m$ 可知 $S_F \setminus \mathbb{F}_{2^m}$ 中元素必落在 $\mathbb{F}_{2^n}$ 真子域中, 通过大小关系得到该集合必定为空, 从而 $S_F = \mathbb{F}_{2^m}$.

(2) 利用高斯和对 $W_{F_a}(b)$ 作 2 进展开, 得到它的 2 赋值最小值为 m. 通过分析首项作为 a, b 的多项式的零点数量, 得到存在 $d_1 j_1 + d_2 j_2 \equiv 0, j_1 + j_2 \equiv 2^n - 2^m \bmod N$.

(3) 比较 wt_2 得到 $j_1 = 2^m j, j_2 = 2^m(2^m - 1 - j)$.

(4) 由陪集分解可知, 当 $s = \gcd(d_1, d_2, N) > 1$ 时, $s \mid (2^m \pm 1) \iff W_{F_a}(0) = \mp 2^m$.

(5) 通过放缩 $S_{F_a}(0)$ 之和得到 $s \mid (2^m - 1)$, 从而 $d_2 - d_1$ 是 $2^m - 1$ 的倍数.

主要思路

(1) 由假设条件 $\ell(n) > m$ 可知 $S_F \setminus \mathbb{F}_{2^m}$ 中元素必落在 $\mathbb{F}_{2^n}$ 真子域中, 通过大小关系得到该集合必定为空, 从而 $S_F = \mathbb{F}_{2^m}$.

(2) 利用高斯和对 $W_{F_a}(b)$ 作 2 进展开, 得到它的 2 赋值最小值为 m. 通过分析首项作为 a, b 的多项式的零点数量, 得到存在 $d_1 j_1 + d_2 j_2 \equiv 0, j_1 + j_2 \equiv 2^n - 2^m \bmod N$.

(3) 比较 wt_2 得到 $j_1 = 2^m j, j_2 = 2^m(2^m - 1 - j)$.

(4) 由陪集分解可知, 当 $s = \gcd(d_1, d_2, N) > 1$ 时, $s \mid (2^m \pm 1) \iff W_{F_a}(0) = \mp 2^m$.

(5) 通过放缩 $S_{F_a}(0)$ 之和得到 $s \mid (2^m - 1)$, 从而 $d_2 - d_1$ 是 $2^m - 1$ 的倍数.

(6) 最后利用同余性质，分类讨论可得.

定理

设 $\ell(n) > m$, $\sigma \circ F = F \circ \sigma$. 若 $\#S_F = 2^m$, 则 $S_F = \mathbb{F}_{2^m}$.

定理

设 $\ell(n) > m$, $\sigma \circ F = F \circ \sigma$. 若 $\#S_F = 2^m$, 则 $S_F = \mathbb{F}_{2^m}$.

由

$$W_{F_{\gamma^2}}(b) = \sum_{x\in\mathbb{F}_{2^n}} \psi(\gamma^2 F(x) + bx) = \sum_{x\in\mathbb{F}_{2^n}} \psi(\gamma^2 F(x^2) + b^{2^n} x^2)$$
$$= \sum_{x\in\mathbb{F}_{2^n}} \psi(\gamma F(x) + b^{2^{n-1}} x) = W_{F_\gamma}(b^{2^{n-1}})$$

可知 S_F 是 σ 不变的.

定理

设 $\ell(n) > m$, $\sigma \circ F = F \circ \sigma$. 若 $\#S_F = 2^m$, 则 $S_F = \mathbb{F}_{2^m}$.

由

$$\begin{aligned} W_{F_{\gamma^2}}(b) &= \sum_{x\in\mathbb{F}_{2^n}} \psi(\gamma^2 F(x) + bx) = \sum_{x\in\mathbb{F}_{2^n}} \psi(\gamma^2 F(x^2) + b^{2^n} x^2) \\ &= \sum_{x\in\mathbb{F}_{2^n}} \psi(\gamma F(x) + b^{2^{n-1}} x) = W_{F_\gamma}(b^{2^{n-1}}) \end{aligned}$$

可知 S_F 是 σ 不变的. 对于 $\gamma \in S_F$, 由 $\ell(n) > m$ 和

$$\dim_{\mathbb{F}_2} \mathbb{F}_2[\sigma]\gamma \leqslant \dim_{\mathbb{F}_2} S_F = m$$

可知 γ 不是 $\mathbb{F}_{2^n}$ 的生成元.

设 $p_1 < p_2 < \cdots < p_l$ 为 m 的奇素因子.

设 $p_1 < p_2 < \cdots < p_l$ 为 m 的奇素因子. 若 $\gamma \in S_F \setminus \mathbb{F}_{2^m}$, 则存在 i 使得 $\gamma \in \mathbb{F}_{2^{n/p_i}} \setminus \mathbb{F}_{2^{m/p_i}}$,

设 $p_1 < p_2 < \cdots < p_l$ 为 m 的奇素因子. 若 $\gamma \in S_F \setminus \mathbb{F}_{2^m}$, 则存在 i 使得 $\gamma \in \mathbb{F}_{2^{n/p_i}} \setminus \mathbb{F}_{2^{m/p_i}}$,

$$\begin{aligned}\#(S_F \setminus \mathbb{F}_{2^m}) &\leqslant \sum_{i=1}^{l}(2^{n/p_i} - 2^{m/p_i}) \leqslant l(2^{n/3} - 2^{m/3}) \\ &< 2^{3^{l-1}-1} \cdot 2^{n/3} \leqslant 2^{m/3-1} \cdot 2^{2m/3} = 2^{m-1}\end{aligned}$$

设 $p_1 < p_2 < \cdots < p_l$ 为 m 的奇素因子. 若 $\gamma \in S_F \setminus \mathbb{F}_{2^m}$, 则存在 i 使得 $\gamma \in \mathbb{F}_{2^{n/p_i}} \setminus \mathbb{F}_{2^{m/p_i}}$,

$$\begin{aligned}\#(S_F \setminus \mathbb{F}_{2^m}) &\leqslant \sum_{i=1}^{l}(2^{n/p_i} - 2^{m/p_i}) \leqslant l(2^{n/3} - 2^{m/3}) \\ &< 2^{3^{l-1}-1} \cdot 2^{n/3} \leqslant 2^{m/3-1} \cdot 2^{2m/3} = 2^{m-1}\end{aligned}$$

而 $S_F \cap \mathbb{F}_{2^m}$ 作为 $\mathbb{F}_{2^m}$ 的真子空间, 大小不超过 2^{m-1}, 二者相加 $\#S_F < 2^m$, 得到矛盾, 从而 $S_F = \mathbb{F}_{2^m}$.

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

对于 p 次本原单位根 ζ, $\zeta^{2^k - 1} = 1 \iff p \mid (2^k - 1)$, 从而 $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}}$, Φ_p 不可约.

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

对于 p 次本原单位根 ζ, $\zeta^{2^k - 1} = 1 \iff p \mid (2^k - 1)$, 从而 $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}}$, Φ_p 不可约.

设 $f_\gamma(x)$ 是 σ 在循环子空间 $\mathbb{F}_2[\sigma]\gamma$ 上的极小多项式.

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

对于 p 次本原单位根 ζ, $\zeta^{2^k - 1} = 1 \iff p \mid (2^k - 1)$, 从而 $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}}$, Φ_p 不可约.

设 $f_\gamma(x)$ 是 σ 在循环子空间 $\mathbb{F}_2[\sigma]\gamma$ 上的极小多项式. 若 γ 是 $\mathbb{F}_{2^n}$ 生成元, 则它不被 $\sigma^p - 1$ 和 $\sigma^2 - 1$ 所零化, 从而 $f_\gamma(x) \nmid (x^p - 1)$, $f_\gamma(x) \nmid (x^2 - 1)$.

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

对于 p 次本原单位根 ζ, $\zeta^{2^k - 1} = 1 \iff p \mid (2^k - 1)$, 从而 $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}}$, Φ_p 不可约.

设 $f_\gamma(x)$ 是 σ 在循环子空间 $\mathbb{F}_2[\sigma]\gamma$ 上的极小多项式. 若 γ 是 $\mathbb{F}_{2^n}$ 生成元, 则它不被 $\sigma^p - 1$ 和 $\sigma^2 - 1$ 所零化, 从而 $f_\gamma(x) \nmid (x^p - 1)$, $f_\gamma(x) \nmid (x^2 - 1)$. 这意味着 $\Phi_p(x)^2 \mid f_\gamma$ 或 $(x-1)^2 \Phi_p(x) \mid f_\gamma$, 从而

$$\ell(\gamma) = \deg f_\gamma \geqslant 2 + (p - 1) = p + 1 > p.$$

注记: 关于条件 $\ell(n) > m$

$\ell(n) > m$ 并不总成立: $\ell(12) = \ell(14) = 5, \ell(18) = 8$, 但我们有:

命题

若 $n = 2p$ 且 2 是模奇素数 p 的原根, 或 $n = 2^k$, 则 $\ell(n) > m$.

$$x^{2p} - 1 = (x^p - 1)^2 = (x-1)^2 \Phi_p(x)^2, \quad \Phi_p(x) := \frac{x^p - 1}{x - 1}.$$

对于 p 次本原单位根 ζ, $\zeta^{2^k - 1} = 1 \iff p \mid (2^k - 1)$, 从而 $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}}$, Φ_p 不可约.

设 $f_\gamma(x)$ 是 σ 在循环子空间 $\mathbb{F}_2[\sigma]\gamma$ 上的极小多项式. 若 γ 是 $\mathbb{F}_{2^n}$ 生成元, 则它不被 $\sigma^p - 1$ 和 $\sigma^2 - 1$ 所零化, 从而 $f_\gamma(x) \nmid (x^p - 1)$, $f_\gamma(x) \nmid (x^2 - 1)$. 这意味着 $\Phi_p(x)^2 \mid f_\gamma$ 或 $(x-1)^2 \Phi_p(x) \mid f_\gamma$, 从而

$$\ell(\gamma) = \deg f_\gamma \geqslant 2 + (p - 1) = p + 1 > p.$$

$n = 2^k$ 情形类似可证.

Stickelberger 定理

设 ω 为 $\mathbb{F}_{2^n}$ 的 Teichmüller 提升,

$$G(\chi) = \sum_{x \in \mathbb{F}_{2^n}^*} \psi(x)\chi(x)$$

为特征 $\chi : \mathbb{F}_{2^n}^* \to \mathbb{C}^\times$ 的高斯和.

设 ω 为 $\mathbb{F}_{2^n}$ 的 Teichmüller 提升,

$$G(\chi) = \sum_{x \in \mathbb{F}_{2^n}^*} \psi(x)\chi(x)$$

为特征 $\chi : \mathbb{F}_{2^n}^* \to \mathbb{C}^\times$ 的高斯和.

定理 (Stickelberger, 1890)

对于 $0 \leqslant i < 2^n - 1$,

$$G(\omega^{-i}) \equiv 2^{\mathrm{wt}_2(i)} \bmod 2^{\mathrm{wt}_2(i)+1}.$$

设 $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, 由高斯和的傅里叶逆变换可得

$$W_{F_a}(b) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} \psi(ax^{d_1} + ax^{d_2} + bx) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} \psi(ax^{d_1})\psi(ax^{d_2})\psi(bx)$$

$$= 1 + N^{-3} \sum_{x \in \mathbb{F}_{2^n}^*} \sum_{j_1,j_2,j_3=0}^{N-1} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{-j_3})\omega^{j_1}(ax^{d_1})\omega^{j_2}(ax^{d_2})\omega^{j_3}(bx)$$

$$= 1 + N^{-3} \sum_{j_1,j_2,j_3=0}^{N-1} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{-j_3})\omega^{j_1+j_2}(a)\omega^{j_3}(b) \sum_{x \in \mathbb{F}_{2^n}^*} \omega^{d_1 j_1 + d_2 j_2 + j_3}(x)$$

$$= 1 + N^{-2} \sum_{j_1,j_2=0}^{N-1} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{d_1 j_1 + d_2 j_2})\omega^{j_1+j_2}(a)\omega^{-d_1 j_1 - d_2 j_2}(b)$$

$$= 1 + N^{-2} \sum_{(j_1,j_2) \neq (0,0)} G(\omega^{-j_1})G(\omega^{-j_2})G(\omega^{d_1 j_1 + d_2 j_2})\omega(a^{j_1+j_2}b^{-d_1 j_1 - d_2 j_2}) - N^{-2}.$$

$W_{F_a}(b)$ 的 2 进展开

设 $\mathcal{J}_{d_1,d_2}$ 是 $\mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$ 中

$$V_{d_1,d_2}(j_1,j_2) := \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) + \mathrm{wt}_2(-d_1 j_1 - d_2 j_2)$$

达到最小值 ν_{d_1,d_2} 的 (j_1,j_2) 集合.

设 $\mathcal{J}_{d_1,d_2}$ 是 $\mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$ 中

$$V_{d_1,d_2}(j_1,j_2) := \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) + \mathrm{wt}_2(-d_1j_1 - d_2j_2)$$

达到最小值 ν_{d_1,d_2} 的 (j_1,j_2) 集合.

$$\begin{aligned} W_{F_a}(b) &= 1 + N^{-2} \sum_{(j_1,j_2) \neq (0,0)} G(\omega^{-j_1}) G(\omega^{-j_2}) G(\omega^{d_1j_1+d_2j_2}) \omega(a^{j_1+j_2} b^{-d_1j_1-d_2j_2}) - N^{-2} \\ &\equiv \sum_{(j_1,j_2) \neq (0,0)} G(\omega^{-j_1}) G(\omega^{-j_2}) G(\omega^{d_1j_1+d_2j_2}) \omega(a^{j_1+j_2} b^{-d_1j_1-d_2j_2}) \bmod 2^n \\ &\equiv 2^{\nu_{d_1,d_2}} \sum_{(j_1,j_2) \in \mathcal{J}_{d_1,d_2}} \omega(a^{j_1+j_2} b^{-(d_1j_1+d_2j_2)}) \bmod 2^{\nu_{d_1,d_2}+1}. \end{aligned}$$

设 $\mathcal{J}_{d_1,d_2}$ 是 $\mathbb{Z}_N \times \mathbb{Z}_N \setminus \{(0,0)\}$ 中

$$V_{d_1,d_2}(j_1,j_2) := \mathrm{wt}_2(j_1) + \mathrm{wt}_2(j_2) + \mathrm{wt}_2(-d_1j_1 - d_2j_2)$$

达到最小值 ν_{d_1,d_2} 的 (j_1,j_2) 集合.

$$\begin{aligned} W_{F_a}(b) &= 1 + N^{-2} \sum_{(j_1,j_2) \neq (0,0)} G(\omega^{-j_1}) G(\omega^{-j_2}) G(\omega^{d_1j_1+d_2j_2}) \omega(a^{j_1+j_2} b^{-d_1j_1-d_2j_2}) - N^{-2} \\ &\equiv \sum_{(j_1,j_2) \neq (0,0)} G(\omega^{-j_1}) G(\omega^{-j_2}) G(\omega^{d_1j_1+d_2j_2}) \omega(a^{j_1+j_2} b^{-d_1j_1-d_2j_2}) \bmod 2^n \\ &\equiv 2^{\nu_{d_1,d_2}} \sum_{(j_1,j_2) \in \mathcal{J}_{d_1,d_2}} \omega(a^{j_1+j_2} b^{-(d_1j_1+d_2j_2)}) \bmod 2^{\nu_{d_1,d_2}+1}. \end{aligned}$$

因此 $v_2(W_{F_a}(b)) \geqslant \nu_{d_1,d_2} \geqslant \dfrac{n}{\max\{\mathrm{wt}_2(d_1), \mathrm{wt}_2(d_2)\}} = m.$

(Moreno 等, 2004)

$W_{F_a}(b)$ 的 2 进展开首项系数

对于 $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, F_a 是弯曲分量, $W_{F_a}(b) = \pm 2^m$, 因此 $\nu_{d_1,d_2} = m$,

$W_{F_a}(b)$ 的 2 进展开首项系数

对于 $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, F_a 是弯曲分量, $W_{F_a}(b) = \pm 2^m$, 因此 $\nu_{d_1,d_2} = m$,

$$W_{F_a}(b) \equiv 2^m \omega(g_a(b)) \bmod 2^{m+1},$$

其中

$$g_a(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2} x^{(-d_1 j_1 - d_2 j_2) \bmod N}.$$

$W_{F_a}(b)$ 的 2 进展开首项系数

对于 $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, F_a 是弯曲分量, $W_{F_a}(b) = \pm 2^m$, 因此 $\nu_{d_1,d_2} = m$,

$$W_{F_a}(b) \equiv 2^m \omega(g_a(b)) \bmod 2^{m+1},$$

其中

$$g_a(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2} x^{(-d_1 j_1 - d_2 j_2) \bmod N}.$$

而多项式 $g_a(x) - 1$ 的次数 $< N$ 但有 2^n 个零点, 从而它是零多项式.

$W_{F_a}(b)$ 的 2 进展开首项系数

对于 $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, F_a 是弯曲分量, $W_{F_a}(b) = \pm 2^m$, 因此 $\nu_{d_1,d_2} = m$,

$$W_{F_a}(b) \equiv 2^m \omega(g_a(b)) \bmod 2^{m+1},$$

其中

$$g_a(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2} x^{(-d_1 j_1 - d_2 j_2) \bmod N}.$$

而多项式 $g_a(x) - 1$ 的次数 $< N$ 但有 2^n 个零点, 从而它是零多项式.

若记

$$h(t) = \sum_{\substack{(j_1,j_2)\in\mathcal{J}_{d_1,d_2} \\ d_1 j_1 + d_2 j_2 \equiv 0 \bmod N}} t^{j_1+j_2},$$

则 $g_a(x) - 1$ 的常数项为 $h(a)$,

$W_{F_a}(b)$ 的 2 进展开首项系数

对于 $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, F_a 是弯曲分量, $W_{F_a}(b) = \pm 2^m$, 因此 $\nu_{d_1,d_2} = m$,

$$W_{F_a}(b) \equiv 2^m \omega(g_a(b)) \bmod 2^{m+1},$$

其中

$$g_a(x) = \sum_{(j_1,j_2)\in\mathcal{J}_{d_1,d_2}} a^{j_1+j_2} x^{(-d_1 j_1 - d_2 j_2) \bmod N}.$$

而多项式 $g_a(x) - 1$ 的次数 $< N$ 但有 2^n 个零点, 从而它是零多项式.

若记

$$h(t) = \sum_{\substack{(j_1,j_2)\in\mathcal{J}_{d_1,d_2} \\ d_1 j_1 + d_2 j_2 \equiv 0 \bmod N}} t^{j_1+j_2},$$

则 $g_a(x) - 1$ 的常数项为 $h(a)$, 作为 a 的多项式有 $2^n - 2^m$ 个零点, 因此它次数至少为 $2^n - 2^m$.

若 $(j_1+j_2) \bmod N \geqslant 2^n-2^m+1$, 则

$$V_{d_1,d_2}(j_1,j_2) \geqslant \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) \geqslant \mathrm{wt}_2(j_1+j_2) = n-\mathrm{wt}_2(-j_1-j_2) \geqslant m+1.$$

若 $(j_1+j_2) \bmod N \geqslant 2^n-2^m+1$, 则

$$V_{d_1,d_2}(j_1,j_2) \geqslant \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) \geqslant \mathrm{wt}_2(j_1+j_2) = n-\mathrm{wt}_2(-j_1-j_2) \geqslant m+1.$$

因此 $h(t)-1$ 的次数恰为 2^n-2^m.

若 $(j_1+j_2) \bmod N \geqslant 2^n-2^m+1$, 则

$$V_{d_1,d_2}(j_1,j_2) \geqslant \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) \geqslant \mathrm{wt}_2(j_1+j_2) = n-\mathrm{wt}_2(-j_1-j_2) \geqslant m+1.$$

因此 $h(t)-1$ 的次数恰为 2^n-2^m. 从而存在 (j_1,j_2) 满足

$$d_1j_1+d_2j_2 \equiv 0, \quad j_1+j_2 \equiv 2^n-2^m \bmod N.$$

若 $(j_1+j_2) \bmod N \geqslant 2^n-2^m+1$, 则

$$V_{d_1,d_2}(j_1,j_2) \geqslant \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) \geqslant \mathrm{wt}_2(j_1+j_2) = n-\mathrm{wt}_2(-j_1-j_2) \geqslant m+1.$$

因此 $h(t)-1$ 的次数恰为 2^n-2^m. 从而存在 (j_1,j_2) 满足

$$d_1j_1+d_2j_2 \equiv 0, \quad j_1+j_2 \equiv 2^n-2^m \bmod N.$$

设

$$j_1=\sum_{a\in S_1}2^a, \quad j_2=\sum_{a\in S_2}2^a, \quad j_1+j_2=\sum_{a\in T}2^a = 2^n-2^m \text{ 或 } 2^{n+1}-2^m-1.$$

其中 $S_1,\ S_2 \subseteq \{0,1,\cdots,n-1\}$,$T=\{m,m+1,\ldots,n-1\}$ 或 $\{0,1,\ldots,m-1,m+1,\ldots,n-1,n\}$.

若 $(j_1+j_2) \bmod N \geqslant 2^n-2^m+1$, 则

$$V_{d_1,d_2}(j_1,j_2) \geqslant \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) \geqslant \mathrm{wt}_2(j_1+j_2) = n-\mathrm{wt}_2(-j_1-j_2) \geqslant m+1.$$

因此 $h(t)-1$ 的次数恰为 2^n-2^m. 从而存在 (j_1,j_2) 满足

$$d_1j_1+d_2j_2 \equiv 0, \quad j_1+j_2 \equiv 2^n-2^m \bmod N.$$

设

$$j_1=\sum_{a\in S_1}2^a, \quad j_2=\sum_{a\in S_2}2^a, \quad j_1+j_2=\sum_{a\in T}2^a = 2^n-2^m \text{ 或 } 2^{n+1}-2^m-1.$$

其中 $S_1,\ S_2 \subseteq \{0,1,\cdots,n-1\}$,$T=\{m,m+1,\ldots,n-1\}$ 或 $\{0,1,\ldots,m-1,m+1,\ldots,n-1,n\}$. 由

$$m=\mathrm{wt}_2(j_1+j_2) \leqslant |T| \leqslant |S_1|+|S_2| = \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) = m$$

可知 $T=\{m,m+1,\ldots,n-1\}=S_1 \sqcup S_2$.

若 $(j_1+j_2) \bmod N \geqslant 2^n-2^m+1$, 则

$$V_{d_1,d_2}(j_1,j_2) \geqslant \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) \geqslant \mathrm{wt}_2(j_1+j_2) = n-\mathrm{wt}_2(-j_1-j_2) \geqslant m+1.$$

因此 $h(t)-1$ 的次数恰为 2^n-2^m. 从而存在 (j_1,j_2) 满足

$$d_1j_1+d_2j_2 \equiv 0, \quad j_1+j_2 \equiv 2^n-2^m \bmod N.$$

设

$$j_1=\sum_{a\in S_1}2^a, \quad j_2=\sum_{a\in S_2}2^a, \quad j_1+j_2=\sum_{a\in T}2^a = 2^n-2^m \text{ 或 } 2^{n+1}-2^m-1.$$

其中 $S_1,\ S_2 \subseteq \{0,1,\cdots,n-1\}$,$T=\{m,m+1,\ldots,n-1\}$ 或 $\{0,1,\ldots,m-1,m+1,\ldots,n-1,n\}$. 由

$$m=\mathrm{wt}_2(j_1+j_2) \leqslant |T| \leqslant |S_1|+|S_2| = \mathrm{wt}_2(j_1)+\mathrm{wt}_2(j_2) = m$$

可知 $T=\{m,m+1,\ldots,n-1\}=S_1 \sqcup S_2$. 从而 $j_1+j_2=(j_1+j_2)_N=2^n-2^m$, 且存在 j 使得 $j_1=2^mj, j_2=2^m(2^m-1-j)$.

引理

假设 $s = \gcd(d_1, d_2, N) > 1$. 若 F 有弯曲分量, 则 s 恰整除 $2^m \pm 1$ 之一, 且

$$s \mid (2^m \pm 1) \iff W_{F_a}(0) = \mp 2^m, \forall a \in \mathbb{F}_{2^n} \setminus S_F.$$

引理

假设 $s = \gcd(d_1, d_2, N) > 1$. 若 F 有弯曲分量, 则 s 恰整除 $2^m \pm 1$ 之一, 且

$$s \mid (2^m \pm 1) \iff W_{F_a}(0) = \mp 2^m, \forall a \in \mathbb{F}_{2^n} \setminus S_F.$$

设 $\mathbb{F}_{2^n}^* = \langle \gamma \rangle, W = \langle \gamma^{N/s} \rangle$, 则 $\mathbb{F}_{2^n}^* = \bigcup_{i=0}^{N/s-1} \gamma^i W$. 由于 $F_a(x)$ 在每个陪集 $\gamma^i W$ 上为常值, 因此

$$W_{F_a}(0) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} \psi\big(F(x)\big) = 1 + s \sum_{i=0}^{N/s-1} \psi\big(F(\gamma^i)\big) \equiv 1 \bmod s.$$

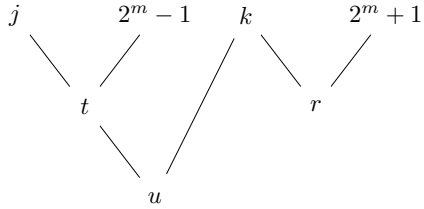
若 F_a 是弯曲分量, 则 $W_{F_a}(0) = \pm 2^m$, 从而命题易得.

存在 $0 \leqslant j \leqslant 2^m - 1$ 使得
$(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$.

存在 $0 \leqslant j \leqslant 2^m - 1$ 使得 $(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$. 设 t, r, u 是对应上方俩个数的最大公因子, 其中 $d_2 - d_1 = k(2^m - 1)/t$.

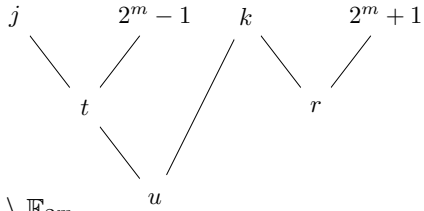
确定 $s \mid (2^m \pm 1)$

存在 $0 \leqslant j \leqslant 2^m - 1$ 使得 $(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$. 设 t, r, u 是对应上方俩个数的最大公因子, 其中 $d_2 - d_1 = k(2^m - 1)/t$.



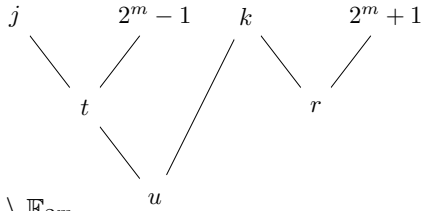
确定 $s \mid (2^m \pm 1)$

存在 $0 \leqslant j \leqslant 2^m - 1$ 使得 $(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$. 设 t, r, u 是对应上方俩个数的最大公因子, 其中 $d_2 - d_1 = k(2^m - 1)/t$.



若 $s \mid (2^m + 1)$, 则 $W_{F_a}(0) = -2^m, \forall a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$,

存在 $0 \leqslant j \leqslant 2^m - 1$ 使得 $(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$. 设 t, r, u 是对应上方俩个数的最大公因子, 其中 $d_2 - d_1 = k(2^m - 1)/t$.



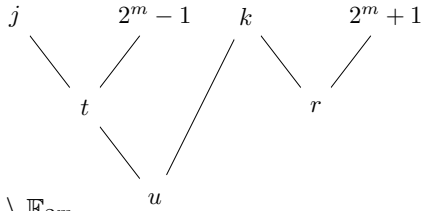
若 $s \mid (2^m + 1)$, 则 $W_{F_a}(0) = -2^m, \forall a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$,

$$\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) = \sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) - \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} W_{F_a}(0) = \sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) + 2^m(2^n - 2^m)$$

$$= \sum_{a\in\mathbb{F}_{2^n}} \sum_{x\in\mathbb{F}_{2^n}} \psi(ax^{d_1} + ax^{d_2}) + 2^m(2^n - 2^m)$$

$$= 2^{3m} + 2^n \#\{x \in \mathbb{F}_{2^n}^* : x^{d_2-d_1} = 1\} = 2^{3m} + 2^n \cdot \frac{(2^m - 1)ur}{t} > 2^{3m}.$$

存在 $0 \leqslant j \leqslant 2^m - 1$ 使得 $(j, 2^m - 1 - j) \in \mathcal{J}_{d_1,d_2}$. 设 t, r, u 是对应上方俩个数的最大公因子, 其中 $d_2 - d_1 = k(2^m - 1)/t$.



若 $s \mid (2^m + 1)$, 则 $W_{F_a}(0) = -2^m, \forall a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$,

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) &= \sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) - \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} W_{F_a}(0) = \sum_{a\in\mathbb{F}_{2^n}} W_{F_a}(0) + 2^m(2^n - 2^m)\\ &= \sum_{a\in\mathbb{F}_{2^n}} \sum_{x\in\mathbb{F}_{2^n}} \psi(ax^{d_1} + ax^{d_2}) + 2^m(2^n - 2^m)\\ &= 2^{3m} + 2^n \#\{x \in \mathbb{F}_{2^n}^* : x^{d_2-d_1} = 1\} = 2^{3m} + 2^n \cdot \frac{(2^m-1)ur}{t} > 2^{3m}.\end{aligned}$$

这不可能, 因此 $s \mid (2^m - 1), r \mid \gcd(s, 2^m + 1) = 1$, $W_{F_a}(0) = 2^m, \forall a \in \mathbb{F}_{2^m}$.

此时

$$\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) = 2^n + 2^n\cdot\frac{(2^m-1)t}{u} - 2^m(2^n-2^m) = 2^n + 2^n(2^m-1)\Big(\frac{u}{t}-1\Big) \leqslant 2^n.$$

此时

$$\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0)=2^n+2^n\cdot\frac{(2^m-1)t}{u}-2^m(2^n-2^m)=2^n+2^n(2^m-1)\Big(\frac{u}{t}-1\Big)\leqslant 2^n.$$

另一方面 ($\mathrm{Tr}:=\mathrm{Tr}_{2^n/2^m}, \psi_m(x):=(-1)^{\mathrm{Tr}_{2^m/2}(x)}$)

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0)&=\sum_{x\in\mathbb{F}_{2^n}}\sum_{a\in\mathbb{F}_{2^m}}\psi_m\big(a\mathrm{Tr}(x^{d_1}+x^{d_2})\big)\\&=2^m\#\{x\in\mathbb{F}_{2^n}:\mathrm{Tr}(x^{d_1}+x^{d_2})=0\}\geqslant 2^n.\end{aligned}$$

此时

$$\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) = 2^n + 2^n\cdot\frac{(2^m-1)t}{u} - 2^m(2^n-2^m) = 2^n + 2^n(2^m-1)\Big(\frac{u}{t}-1\Big) \leqslant 2^n.$$

另一方面 ($\mathrm{Tr} := \mathrm{Tr}_{2^n/2^m}, \psi_m(x) := (-1)^{\mathrm{Tr}_{2^m/2}(x)}$)

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^m}} W_{F_a}(0) &= \sum_{x\in\mathbb{F}_{2^n}}\sum_{a\in\mathbb{F}_{2^m}} \psi_m\big(a\mathrm{Tr}(x^{d_1}+x^{d_2})\big)\\ &= 2^m\#\{x\in\mathbb{F}_{2^n} : \mathrm{Tr}(x^{d_1}+x^{d_2})=0\} \geqslant 2^n.\end{aligned}$$

因此 $t=u$, $d_2-d_1 = \dfrac{k}{u}(2^m-1)$ 是 2^m-1 的倍数.

不妨设 $d_1 = 1 + 2^l, d_2 = 2^{k_1} + 2^{k_2}$, 其中 $0 < l < m, 0 \leqslant k_1 < k_2 < n, d_1 < d_2$.

不妨设 $d_1 = 1 + 2^l, d_2 = 2^{k_1} + 2^{k_2}$, 其中 $0 < l < m, 0 \leqslant k_1 < k_2 < n, d_1 < d_2$. 我们有 $\mathrm{wt}_2(d_2 - d_1) = \mathrm{wt}_2((2^m - 1)k) = m$.

不妨设 $d_1 = 1 + 2^l, d_2 = 2^{k_1} + 2^{k_2}$, 其中 $0 < l < m, 0 \leqslant k_1 < k_2 < n, d_1 < d_2$. 我们有 $\mathrm{wt}_2(d_2 - d_1) = \mathrm{wt}_2((2^m - 1)k) = m$.

假设 $l < k_1$, 则

$$d_2 - d_1 = 2^{k_1} - 1 + 2^{k_2} - 2^l = 1 + 2 + \cdots + 2^{l-1} + 2^{l+1} + \cdots + 2^{k_1 - 1} + 2^{k_2}$$

且 $m = \mathrm{wt}_2(d_2 - d_1) = k_1$.

不妨设 $d_1 = 1 + 2^l, d_2 = 2^{k_1} + 2^{k_2}$, 其中 $0 < l < m, 0 \leqslant k_1 < k_2 < n, d_1 < d_2$. 我们有 $\mathrm{wt}_2(d_2 - d_1) = \mathrm{wt}_2((2^m - 1)k) = m$.

假设 $l < k_1$, 则

$$d_2 - d_1 = 2^{k_1} - 1 + 2^{k_2} - 2^l = 1 + 2 + \cdots + 2^{l-1} + 2^{l+1} + \cdots + 2^{k_1 - 1} + 2^{k_2}$$

且 $m = \mathrm{wt}_2(d_2 - d_1) = k_1$. 由于 $d_2 - d_1 = (2^m - 1) + (2^{k_2} - 2^l)$ 是 $2^m - 1$ 的倍数, 因此 $k_2 = m + l$,

$$d_1 = 1 + 2^l, \qquad d_2 = 2^m + 2^{m+l} = 2^m d_1,$$

不妨设 $d_1 = 1 + 2^l, d_2 = 2^{k_1} + 2^{k_2}$, 其中 $0 < l < m, 0 \leqslant k_1 < k_2 < n, d_1 < d_2$. 我们有 $\mathrm{wt}_2(d_2 - d_1) = \mathrm{wt}_2((2^m - 1)k) = m$.

假设 $l < k_1$, 则

$$d_2 - d_1 = 2^{k_1} - 1 + 2^{k_2} - 2^l = 1 + 2 + \cdots + 2^{l-1} + 2^{l+1} + \cdots + 2^{k_1 - 1} + 2^{k_2}$$

且 $m = \mathrm{wt}_2(d_2 - d_1) = k_1$. 由于 $d_2 - d_1 = (2^m - 1) + (2^{k_2} - 2^l)$ 是 $2^m - 1$ 的倍数, 因此 $k_2 = m + l$,

$$d_1 = 1 + 2^l, \qquad d_2 = 2^m + 2^{m+l} = 2^m d_1,$$

但此时不难证明 $F_a, a \in \mathbb{F}_{2^m}$ 或 $\mathrm{Tr}^{-1}(1)$ 均非弯曲, 从而没有最大弯曲分量数.

故 $k_1 \leqslant l \leqslant k_2$,

$$d_2 - d_1 = 1 + 2 + \cdots + 2^{k_1-1} + 2^l + 2^{l+1} + \cdots + 2^{k_2-1}$$

且 $\mathrm{wt}_2(d_2 - d_1) = k_1 + k_2 - l = m$.

故 $k_1 \leqslant l \leqslant k_2$,

$$d_2 - d_1 = 1 + 2 + \cdots + 2^{k_1-1} + 2^l + 2^{l+1} + \cdots + 2^{k_2-1}$$

且 $\mathrm{wt}_2(d_2 - d_1) = k_1 + k_2 - l = m$. 由

$$d_2 - d_1 = 2^{m+l-k_1} + 2^{k_1} - 2^l - 1 = 2^{l-k_1}(2^m - 1) + (2^{k_1} - 1)(1 - 2^{l-k_1})$$

可知 $(2^{k_1} - 1)(2^{l-k_1} - 1) < 2^m - 1$ 被 $2^m - 1$ 整除.

故 $k_1 \leqslant l \leqslant k_2$,

$$d_2 - d_1 = 1 + 2 + \cdots + 2^{k_1-1} + 2^l + 2^{l+1} + \cdots + 2^{k_2-1}$$

且 $\mathrm{wt}_2(d_2 - d_1) = k_1 + k_2 - l = m$. 由

$$d_2 - d_1 = 2^{m+l-k_1} + 2^{k_1} - 2^l - 1 = 2^{l-k_1}(2^m - 1) + (2^{k_1} - 1)(1 - 2^{l-k_1})$$

可知 $(2^{k_1} - 1)(2^{l-k_1} - 1) < 2^m - 1$ 被 $2^m - 1$ 整除. 故 $k_1 = 0$ 或 l.

故 $k_1 \leqslant l \leqslant k_2$,

$$d_2 - d_1 = 1 + 2 + \cdots + 2^{k_1-1} + 2^l + 2^{l+1} + \cdots + 2^{k_2-1}$$

且 $\mathrm{wt}_2(d_2 - d_1) = k_1 + k_2 - l = m$. 由

$$d_2 - d_1 = 2^{m+l-k_1} + 2^{k_1} - 2^l - 1 = 2^{l-k_1}(2^m - 1) + (2^{k_1} - 1)(1 - 2^{l-k_1})$$

可知 $(2^{k_1} - 1)(2^{l-k_1} - 1) < 2^m - 1$ 被 $2^m - 1$ 整除. 故 $k_1 = 0$ 或 l.

若 $k_1 = l$, 则

$$F(x) = x^{1+2^l} + x^{2^l+2^m}.$$

故 $k_1 \leqslant l \leqslant k_2$,

$$d_2 - d_1 = 1 + 2 + \cdots + 2^{k_1-1} + 2^l + 2^{l+1} + \cdots + 2^{k_2-1}$$

且 $\mathrm{wt}_2(d_2 - d_1) = k_1 + k_2 - l = m$. 由

$$d_2 - d_1 = 2^{m+l-k_1} + 2^{k_1} - 2^l - 1 = 2^{l-k_1}(2^m - 1) + (2^{k_1} - 1)(1 - 2^{l-k_1})$$

可知 $(2^{k_1} - 1)(2^{l-k_1} - 1) < 2^m - 1$ 被 $2^m - 1$ 整除. 故 $k_1 = 0$ 或 l.

若 $k_1 = l$, 则

$$F(x) = x^{1+2^l} + x^{2^l+2^m}.$$

若 $k_1 = 0$, 则

$$F(x) = x^{1+2^l} + x^{1+2^{l+m}} \text{ 仿射等价 } x^{2^{m-l}+2^m} + x^{1+2^{m-l}}.$$

我们来估计**非线性度** $\mathcal{N}_F$.

我们来估计**非线性度** $\mathcal{N}_F$.

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^n}} W_{F_a}^2(0) &= \sum_{x,y\in\mathbb{F}_{2^n}} \psi\Big(a(F(x)+F(y))\Big)\\ &= 2^n \#\{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n} : F(x)=F(y)\}\\ &= 2^n \sum_{b\in\mathrm{Im}(F)} \big(\#F^{-1}(b)\big)^2 \geqslant \frac{2^n}{\#\,\mathrm{Im}(F)}\left(\sum_{b\in\mathrm{Im}(F)} \#F^{-1}(b)\right)^2 \quad \text{(柯西不等式)}\\ &= \frac{2^{3n}}{\#\,\mathrm{Im}(F)}.\end{aligned}$$

从而

$$\sum_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0) = \sum_{a\in\mathbb{F}_{2^n}} W_{F_a}^2(0) - 2^{2n} - 2^n(2^n - 2^m)$$

($a=0$ 部分 ↓　　F_a 弯曲 ↓)

$$\geqslant \frac{2^{3n}}{\#\,\mathrm{Im}(F)} - 2^{2n+1} + 2^{n+m}.$$

从而

$$\sum_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0) = \sum_{a\in\mathbb{F}_{2^n}} W_{F_a}^2(0) - 2^{2n} - 2^n(2^n - 2^m)$$

$$\geqslant \frac{2^{3n}}{\#\operatorname{Im}(F)} - 2^{2n+1} + 2^{n+m}.$$

$a=0$ 部分 ↓　　F_a 弯曲 ↓

设 $T := \#\{a \in \mathbb{F}_{2^m}^* : W_{F_a}(0) \neq 0\}$, 那么

$$\max_{a\in\mathbb{F}_{2^m}^*, v\in\mathbb{F}_{2^n}} W_{F_a}^2(v) \geqslant \max_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0) \geqslant \frac{1}{T}\sum_{a\in\mathbb{F}_{2^m}^*} W_{F_a}^2(0),$$

$$\mathcal{N}_F := 2^{n-1} - \frac{1}{2}\max_{a\neq 0,\omega} |W_{F_a}(\omega)| \leqslant 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{3m}}{T}\left(\frac{2^{3m}}{\#\operatorname{Im}(F)} - 2^{m+1} + 1\right)}$$

差分均匀度估计

设

$$\Delta = \{x + y : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n},\ x \neq y,\ F(x) = F(y)\}.$$

设

$$\Delta = \{x + y : (x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n},\ x \neq y,\ F(x) = F(y)\}.$$

差分均匀度估计通过

$$\begin{aligned}\delta_F &= \max_{a \neq 0, b} \#\{x : F(x+a) + F(x) = b\} \geqslant \frac{1}{\#\Delta} \sum_{a \in \mathbb{F}_{2^n}^*} \#\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = 0\} \\ &= \frac{1}{\#\Delta}\Big(\#\{(x, y) : F(x) = F(y)\} - 2^n\Big) \\ &= \frac{1}{\#\Delta}\Big(\sum_{b \in \mathrm{Im}(F)} \big(\#F^{-1}(b)\big)^2 - 2^n\Big) \geqslant \frac{1}{\#\Delta}\Big(\frac{2^{2n}}{\#\,\mathrm{Im}(F)} - 2^n\Big).\end{aligned}$$

二项式情形映射 F 的特点

最后, 我们来考虑 $F(x) = x^{2^l+1} + x^{2^l+2^m}$ 情形下 $\mathcal{N}_F$ 的估计.

最后, 我们来考虑 $F(x)=x^{2^l+1}+x^{2^l+2^m}$ 情形下 $\mathcal{N}_F$ 的估计.

定理

设 $F(x)=x^{2^l+1}+x^{2^l+2^m}$, $d=\gcd(l,m)$,

$$s:=\gcd(2^l+1,2^l+2^m,N)=\gcd(2^l+1,2^m-1)=\begin{cases}1, & \text{若 } v_2(m)\leqslant v_2(l);\\ 2^d+1, & \text{若 } v_2(m)>v_2(l).\end{cases}$$

那么 F 在 $\mathbb{F}_{2^m}$ 上恒为零; 在 $\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$ 上是到

$$\{y\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}:\mathrm{Tr}_{2^n/2^m}(y)\in(\mathbb{F}_{2^m}^*)^s\}.$$

的 $s:1$ 的满射.

二项式情形映射 F 的特点 (续)

证明

显然 $F(x) = 0, \forall x \in \mathbb{F}_{2^m}$.

二项式情形映射 F 的特点 (续)

证明

显然 $F(x)=0, \forall x \in \mathbb{F}_{2^m}$.

设 $\mathrm{Tr}=\mathrm{Tr}_{2^n/2^m}$. 若 $F(x)=x^{2^l}\mathrm{Tr}(x)=y \notin \mathbb{F}_{2^m}$, 则

$$\mathrm{Tr}(y^{2^{n-l}})=\mathrm{Tr}\big(x\mathrm{Tr}(x)^{2^{n-l}}\big)=\mathrm{Tr}(x)^{1+2^{n-l}} \in D := (\mathbb{F}_{2^m}^*)^{1+2^{n-l}}.$$

二项式情形映射 F 的特点 (续)

证明

显然 $F(x)=0, \forall x \in \mathbb{F}_{2^m}$.

设 $\mathrm{Tr}=\mathrm{Tr}_{2^n/2^m}$. 若 $F(x)=x^{2^l}\mathrm{Tr}(x)=y \notin \mathbb{F}_{2^m}$, 则

$$\mathrm{Tr}(y^{2^{n-l}})=\mathrm{Tr}(x\mathrm{Tr}(x)^{2^{n-l}})=\mathrm{Tr}(x)^{1+2^{n-l}} \in D:=(\mathbb{F}_{2^m}^*)^{1+2^{n-l}}.$$

由于

$$\gcd(2^{n-l}+1,2^m-1)=\gcd(2^l+1,2^m-1)=s,$$

因此 $D=(\mathbb{F}_{2^m}^*)^s$.

二项式情形映射 F 的特点 (续)

证明

显然 $F(x)=0, \forall x \in \mathbb{F}_{2^m}$.

设 $\mathrm{Tr}=\mathrm{Tr}_{2^n/2^m}$. 若 $F(x)=x^{2^l}\mathrm{Tr}(x)=y \notin \mathbb{F}_{2^m}$, 则

$$\mathrm{Tr}(y^{2^{n-l}})=\mathrm{Tr}(x\mathrm{Tr}(x)^{2^{n-l}})=\mathrm{Tr}(x)^{1+2^{n-l}} \in D:=(\mathbb{F}_{2^m}^*)^{1+2^{n-l}}.$$

由于

$$\gcd(2^{n-l}+1,2^m-1)=\gcd(2^l+1,2^m-1)=s,$$

因此 $D=(\mathbb{F}_{2^m}^*)^s$.

反之, 若 $\mathrm{Tr}(y^{2^{n-l}})=u^{1+2^{n-l}}$, 则 $\mathrm{Tr}(x)=u\zeta, \zeta \in \mu_{1+2^{n-l}}=\mu_s$.

二项式情形映射 F 的特点 (续)

证明

显然 $F(x)=0, \forall x \in \mathbb{F}_{2^m}$.

设 $\mathrm{Tr}=\mathrm{Tr}_{2^n/2^m}$. 若 $F(x)=x^{2^l}\mathrm{Tr}(x)=y \notin \mathbb{F}_{2^m}$, 则

$$\mathrm{Tr}(y^{2^{n-l}})=\mathrm{Tr}(x\mathrm{Tr}(x)^{2^{n-l}})=\mathrm{Tr}(x)^{1+2^{n-l}} \in D:=(\mathbb{F}_{2^m}^*)^{1+2^{n-l}}.$$

由于

$$\gcd(2^{n-l}+1, 2^m-1)=\gcd(2^l+1, 2^m-1)=s,$$

因此 $D=(\mathbb{F}_{2^m}^*)^s$.

反之, 若 $\mathrm{Tr}(y^{2^{n-l}})=u^{1+2^{n-l}}$, 则 $\mathrm{Tr}(x)=u\zeta, \zeta \in \mu_{1+2^{n-l}}=\mu_s$. 从而

$$x=\left(\frac{y}{\mathrm{Tr}(x)}\right)^{2^{n-l}}=\left(\frac{y}{u\zeta}\right)^{2^{n-l}}=\frac{\zeta y^{2^{n-l}}}{u^{2^{n-l}}} \in F^{-1}(y). \qquad \square$$

二项式情形的 $\mathcal{N}_F$ 的估计

定理

设 $F(x) = x^{2^l+1} + x^{2^l+2^m}$，则

$$\mathcal{N}_F \leqslant \begin{cases} 2^{n-1} - 2^{m-1}, & \text{若 } v_2(m) \leqslant v_2(l); \\ 2^{n-1} - 2^{\frac{3m}{2}+d-1}, & \text{若 } v_2(m) > v_2(l). \end{cases}$$

二项式情形的 $\mathcal{N}_F$ 的估计

定理

设 $F(x) = x^{2^l+1} + x^{2^l+2^m}$，则

$$\mathcal{N}_F \leqslant \begin{cases} 2^{n-1} - 2^{m-1}, & \text{若 } v_2(m) \leqslant v_2(l); \\ 2^{n-1} - 2^{\frac{3m}{2}+d-1}, & \text{若 } v_2(m) > v_2(l). \end{cases}$$

我们需要如下结果来帮助计算 $W_{F_a}(0)$.

定理 (Coulter, 1999)

$$\sum_{z\in\mathbb{F}_{2^m}} \psi_m(az^s) = \begin{cases} 0, & \text{若 } v_2(m) \leqslant v_2(l); \\ (-1)^{\frac{m}{2d}} 2^{\frac{m}{2}}, & \text{若 } v_2(m) > v_2(l), a \in \mathbb{F}_{2^m}^* \setminus (\mathbb{F}_{2^m}^*)^s; \\ -(-1)^{\frac{m}{2d}} 2^{\frac{m}{2}+d}, & \text{若 } v_2(m) > v_2(l), a \in (\mathbb{F}_{2^m}^*)^s. \end{cases}$$

二项式情形的 $\mathcal{N}_F$ 的估计: $a \notin \mathbb{F}_{2^m}$

证明

若 $\beta \in \mathbb{F}_{2^n}$ 满足 $\mathrm{Tr}(\beta) = 1$, 则 $\mathbb{F}_{2^n} = \mathbb{F}_{2^m} + \mathbb{F}_{2^m}\beta$.

二项式情形的 $\mathcal{N}_F$ 的估计: $a \notin \mathbb{F}_{2^m}$

证明

若 $\beta \in \mathbb{F}_{2^n}$ 满足 $\mathrm{Tr}(\beta) = 1$, 则 $\mathbb{F}_{2^n} = \mathbb{F}_{2^m} + \mathbb{F}_{2^m}\beta$. 设 $a \neq 0$, 则

$$
\begin{aligned}
W_{F_a}(0) &= \sum_{v\in\mathbb{F}_{2^n}} \psi\big(aF(v)\big) = 2^m + \sum_{v\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \psi\big(aF(v)\big) \\
&= 2^m + s \sum_{\mathrm{Tr}(y)\in(\mathbb{F}_{2^m}^*)^s} \psi(ay) = 2^m + \sum_{\chi^s=1} \sum_{y\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \psi(ay)\chi\big(\mathrm{Tr}(y)\big) \\
&= 2^m + \sum_{\chi^s=1} \sum_{x\in\mathbb{F}_{2^m}} \sum_{u\in\mathbb{F}_{2^m}^*} \psi\big(a(x+\beta u)\big)\chi(u) \\
&= 2^m + \sum_{\chi^s=1} \left(\sum_{x\in\mathbb{F}_{2^m}} \psi(ax) \cdot \sum_{u\in\mathbb{F}_{2^m}^*} \psi(a\beta u)\chi(u) \right).
\end{aligned}
$$

证明

若 $\beta \in \mathbb{F}_{2^n}$ 满足 $\mathrm{Tr}(\beta) = 1$, 则 $\mathbb{F}_{2^n} = \mathbb{F}_{2^m} + \mathbb{F}_{2^m}\beta$. 设 $a \neq 0$, 则

$$\begin{aligned} W_{F_a}(0) &= \sum_{v\in\mathbb{F}_{2^n}} \psi\big(aF(v)\big) = 2^m + \sum_{v\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \psi\big(aF(v)\big) \\ &= 2^m + s \sum_{\mathrm{Tr}(y)\in(\mathbb{F}_{2^m}^*)^s} \psi(ay) = 2^m + \sum_{\chi^s=1} \sum_{y\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \psi(ay)\chi\big(\mathrm{Tr}(y)\big) \\ &= 2^m + \sum_{\chi^s=1} \sum_{x\in\mathbb{F}_{2^m}} \sum_{u\in\mathbb{F}_{2^m}^*} \psi\big(a(x+\beta u)\big)\chi(u) \\ &= 2^m + \sum_{\chi^s=1} \left(\sum_{x\in\mathbb{F}_{2^m}} \psi(ax) \cdot \sum_{u\in\mathbb{F}_{2^m}^*} \psi(a\beta u)\chi(u) \right). \end{aligned}$$

若 $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, 则 $\sum_{x\in\mathbb{F}_{2^m}} \psi(ax) = \sum_{x\in\mathbb{F}_{2^m}} \psi_m\big(\mathrm{Tr}(a)x\big) = 0$, 从而 $W_{F_a}(0) = 2^m$.

续证

若 $a \in \mathbb{F}_{2^m}^*$, 则

$$\begin{aligned} W_{F_a}(0) &= 2^m + s \sum_{\mathrm{Tr}(y) \in (\mathbb{F}_{2^m}^*)^s} \psi(ay) \\ &= 2^m + s2^m \sum_{z \in (\mathbb{F}_{2^m}^*)^s} \psi_m(az) = 2^m \sum_{z \in \mathbb{F}_{2^m}} \psi_m(az^s). \end{aligned}$$

续证

若 $a \in \mathbb{F}_{2^m}^*$, 则

$$\begin{aligned} W_{F_a}(0) &= 2^m + s \sum_{\mathrm{Tr}(y) \in (\mathbb{F}_{2^m}^*)^s} \psi(ay) \\ &= 2^m + s2^m \sum_{z \in (\mathbb{F}_{2^m}^*)^s} \psi_m(az) = 2^m \sum_{z \in \mathbb{F}_{2^m}} \psi_m(az^s). \end{aligned}$$

由 *Coulter* 的结果可得 $W_{F_a}(0)$, 从而得到 $\mathcal{N}_F \leqslant 2^{n-1} - \frac{1}{2} \max_{a \neq 0} |W_{F_a}(0)|$ 的估计:

$$W_{F_a}(0) = \begin{cases} 2^n, & \text{若 } a = 0; \\ 2^m, & \text{若 } a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}; \\ 0, & \text{若 } v_2(m) \leqslant v_2(l); \\ (-1)^{\frac{m}{2d}} 2^{\frac{3m}{2}}, & \text{若 } v_2(m) > v_2(l), a \in \mathbb{F}_{2^m}^* \setminus (\mathbb{F}_{2^m}^*)^s; \\ -(-1)^{\frac{m}{2d}} 2^{\frac{3m}{2}+d}, & \text{若 } v_2(m) > v_2(l), a \in (\mathbb{F}_{2^m}^*)^s. \end{cases}$$

□


謝　謝